3-17-2021

A Cyber-Physical Anomaly Detection for Wide-Area Protection using Machine Learning

Vivek Kumar Singh
Idaho National Laboratory

Manimaran Govindarasu
Iowa State University, gmani@iastate.edu

A Cyber-Physical Anomaly Detection for Wide-Area Protection using Machine Learning

Abstract

Wide-area protection scheme (WAPS) provides system-wide protection by detecting and mitigating small and large-scale disturbances that are difficult to resolve using local protection schemes. As this protection scheme is evolving from a substation-based distributed remedial action scheme (DRAS) to the control center-based centralized RAS (CRAS), it presents severe challenges to their cybersecurity because of its heavy reliance on an insecure grid communication, and its compromise would lead to system failure. This paper presents an architecture and methodology for developing a cyber-physical anomaly detection system (CPADS) that utilizes synchrophasor measurements and properties of network packets to detect data integrity and communication failure attacks on measurement and control signals in CRAS. The proposed machine leaning-based methodology applies a rules-based approach to select relevant input features, utilizes variational mode decomposition (VMD) and decision tree (DT) algorithms to develop multiple classification models, and performs final event identification using a rules-based decision logic. We have evaluated the proposed methodology of CPADS using the IEEE 39 bus system for several performance measures (accuracy, recall, precision, and F-measure) in a cyber-physical testbed environment. Our experimental results reveal that the proposed algorithm (VMD-DT) of CPADS outperforms the existing machine learning classifiers during noisy and noise-free measurements while incurring an acceptable processing overhead.

Keywords

Wide-area protection, cybersecurity, synchrophasor, machine learning, variational mode decomposition

Disciplines

Power and Energy

Comments

This is a manuscript of an article published as Singh, Vivek Kumar, and Manimaran Govindarasu. "A Cyber-Physical Anomaly Detection for Wide-Area Protection using Machine Learning." *IEEE Transactions on Smart Grid* (2021). DOI: 10.1109/TSG.2021.3066316. Posted with permission.

A Cyber-Physical Anomaly Detection for Wide-Area Protection using Machine Learning

Vivek Kumar Singh, *Member, IEEE,* and Manimaran Govindarasu, *Fellow, IEEE,*

***Abstract*—Wide-area protection scheme (WAPS) provides system-wide protection by detecting and mitigating small and large-scale disturbances that are difficult to resolve using local protection schemes. As this protection scheme is evolving from a substation-based distributed remedial action scheme (DRAS) to the control center-based centralized RAS (CRAS), it presents severe challenges to their cybersecurity because of its heavy reliance on an insecure grid communication, and its compromise would lead to system failure. This paper presents an architecture and methodology for developing a cyber-physical anomaly detection system (CPADS) that utilizes synchrophasor measurements and properties of network packets to detect data integrity and communication failure attacks on measurement and control signals in CRAS. The proposed machine leaning-based methodology applies a rules-based approach to select relevant input features, utilizes variational mode decomposition (VMD) and decision tree (DT) algorithms to develop multiple classification models, and performs final event identification using a rules-based decision logic. We have evaluated the proposed methodology of CPADS using the IEEE 39 bus system for several performance measures (accuracy, recall, precision, and F-measure) in a cyber-physical testbed environment. Our experimental results reveal that the proposed algorithm (VMD-DT) of CPADS outperforms the existing machine learning classifiers during noisy and noise-free measurements while incurring an acceptable processing overhead.**

***Index Terms*—Wide-area protection, cybersecurity, synchrophasor, machine learning, variational mode decomposition.**

I. Introduction

TODAY'S electric power grid has transformed into a highly complex and interconnected cyber-physical system (CPS) and numerous controllers are operating at substation and control center levels to maintain the stability and reliability of power system. The significant growth in cyber technologies to make the grid *smarter* has driven the energy industry to a new era of reliability, sustainability, and efficiency, which require a higher dependence on communication infrastructure, data sharing devices, and sophisticated wide-area controllers. While the emergence of CPS forms a core modus operandi of the modern power grid, it has also rendered the grid network increasingly vulnerable to numerous cyberattacks [1], [2]. The past cybersecurity incidents, including the Stuxnet Worm [3] and Ukraine grid hack [4] in 2015 and 2016, have shown that the grid operation and physical infrastructures can be compromised due to cyberattacks—such as injecting malware, data spoofing, denial of service (DoS) attack, etc.

Wide-area protection scheme (WAPS), also known as a remedial action scheme (RAS) or special protection scheme (SPS), is one of the critical wide-area protection and control (WAPAC) applications that provides a system-wide protection with optimized and coordinated control actions. Significant efforts in the past have shown how the design and development of RAS have shifted from a substation-based distributed to the control center-based centralized protection scheme [5]-[8]. The Southern California Edison (SCE) has developed a CRAS as an optimized and economical solution over substation-based local protection schemes to mitigate transmission line overloading while minimizing maintenance costs [7], [8]. Besides, there has been a rapid shift in incorporating phasor measurement unit (PMU) measurements to develop mission-critical applications, such as CRAS based on the dynamic stability assessment [6], [9], [10]. The authors of [6] discuss the emerging trends, design, and architecture of synchrophasor-based WAPS for several applications, including frequency instability, voltage instability, oscillation monitoring, thermal overloading, and a combination of these applications. The North American Electric Reliability Corporation (NERC) presents a response-based CRAS, deployed in the Bonneville Power Administration (BPA)'s control center, which relies on synchrophasors for wide-area stability and voltage control [9], [10].

A. Motivation

With the objective of pushing PMU applications from mission-supportive to mission-critical, PMUs are increasingly applied to develop WAPS. In [11], the authors proposed a PMU-based CRAS for predicting catastrophic power system events using ensemble decision trees. In [12], the authors presented an artificial neural network (ANN)-based WAPS for predicting and mitigating transient stability using PMU measurements. In a similar context, the authors of [13] discussed an adaptive scheme based on transient energy analysis and tested the proposed approach using the IEEE 39 bus system. Although significant efforts, previous research [11]-[13] assumed that the synchrophasor and SCADA networks are secure and reliable and did not consider the cybersecurity aspects associated with the grid services.

The current breakthrough solution—CRAS [8] is an ideal target for attackers as its compromise would lead to a single point of failure in control center-based protection function. Since the CRAS is conventionally designed to mitigate power system disturbances and not handle unexpected cyberattacks, any unusual malfunction, triggered through cyberattacks, can

Vivek Kumar Singh is with the Department of Power and Energy Systems, Idaho National Laboratory (INL), Idaho Falls, ID, 83415 USA (e-mail: vivekkumar.singh@inl.gov).

Manimaran Govindarasu is with the Department of Electrical and Computer Engineering, Iowa State University, Ames, IA 50011 USA (email:gmani@iastate.edu)

affect the operational reliability and stability of the system. Further, it relies heavily on insecure grid networks that is exposed to countless cyberattacks. Some research efforts in the past have shown how the critical application like WAPS is subjected to stealthy cyberattacks [14]-[15]. In [14], the authors discussed the vulnerability assessment of SCADA communication protocols, and showed the impact analysis of a coordinated cyberattack on the transient voltage stability in RAS. The authors of [15] illustrated how the malware-initiated stealthy and coordinated cyberattacks can severely impact the system generator while targeting the RAS operation. The existing literature [18]-[21] in the WAPAC cybersecurity domain mostly addresses limited attack surfaces on either measurement or control-signals. Therefore, it is imperative to analyze cyberattack surfaces in spatial and temporal levels on both measurements and control signals and eventually develop a defense-in-depth architecture to enhance the resiliency of CRAS against cyber threats. In our previous works, we have performed the impact analysis of stealthy cyberattacks on control signals [15] and illustrated how the decision tree (DT) could be utilized in detecting malicious tripping attack in CRAS [16].

B. Related Work

Over the recent decade, with the emergence of the smart grid, researchers with different backgrounds have proposed various types of anomaly detection systems (ADS), including model-based, multi-agent, protocol-specific, and machine learning-based ADS for the cyber-physical security of WAPAC. In [17], the authors proposed a model-based ADS for detecting data integrity attacks on measurement signals in the automatic generation control (AGC); however, the proposed method may fail to detect multi-layer stealthy anomalies on measurement and control signals. Also, applying redundant measurements, such as load forecast to detect anomalies is unfit in CRAS as the forecast error may amplify during the unplanned outages [18]. The authors of [19] and [20] presented a multi-agent-based ADS to detect cyberattacks while focusing on local protection scheme and DRAS. In [21]-[23], the authors discussed a specification-based ADS for supervisory control and data acquisition (SCADA) and synchrophasor communication protocols. Although the proposed signature-based ADSs perform well in detecting anomalies using network packet logs, they require an intensive knowledge of communication protocols for developing rules; and hence not appropriate for the big-data problem. Further, they may fail to detect physical disturbances, such as line faults, making it unfit for the CRAS cybersecurity.

Several research efforts [24]-[26] have shown the application of machine learning and data mining techniques in developing the ADS for wide-area monitoring system (WAMS), including frequency, voltage, and power oscillation monitoring while considering anomalies on incoming measurement signals. Pan et al. presented a common path mining-based ADS to classify cyberattacks, normal operations, and physical disturbances using synchrophasor measurements and audit logs and tested the proposed method on a smaller three-bus two-line transmission system [27]. However, the applied common path mining method requires human efforts and lacks fast detection with limited applications. Since the accuracy of machine learning classifiers depends on input features, several techniques have been proposed to select relevant features for the accurate classification of different events. The authors of [28]-[30] presented how system parameters, such as voltage, current, frequency, and their computed derivative features could be utilized in developing decision tree-based efficient classifiers for detecting power system events. Cyber-physical events in power systems create different flavors of transient phenomena that can be detected using the computed derivative features from raw PMU data.

Recently, a novel signal decomposition technique, called variational mode decomposition (VMD) [31], is introduced that decomposes a multi-component signal into the set of sub-signal modes. Previous research efforts have demonstrated its application in performing multi-level classifications [31], [32] and illustrated its superior performance compared to the conventional empirical mode decomposition (EMD) technique; however, they provide very little insight or discussion related to its application in the CRAS cybersecurity. Recently, the authors of [33] discussed how the VMD technique could be applied to detect false data injection attack (FDI) in the state estimation; however, the proposed method is not applicable in detecting other types of attacks, such as communication failure attacks and coordinated attacks. Motivated by its excellent capability to extract relevant features and the best of our knowledge, this is the first work that applies the VMD technique to develop a CPADS that characterizes different types of events, including cyberattacks, physical disturbances, and normal operation in the context of synchrophasor-based WAPS. Also, there has been no prior work in detecting coordinated cyberattacks in CRAS cybersecurity.

C. Contribution

The key contributions of this paper include:

1) Novel architecture and methodology are proposed for developing the CPADS by leveraging PMU measurements and network packet properties and applying VMD and DT algorithms.

2) Rules-based feature selection method is proposed by applying the filter and wrapper methods to obtain relevant features for machine learning-based classifiers.

3) A detailed performance analysis, during both cyber and physical events, in a hardware-in-the-loop (HIL) cyber-physical security testbed environment is presented.

The rest of the paper is organized as follows: Section II presents a brief overview of different cyberattacks and introduces the problem formulation in CRAS cybersecurity. The proposed architecture and machine learning-based methodology are presented in Section III. Section IV and Section V present a case study and experimental evaluation of the proposed algorithm on IEEE 39 bus system. Section VI provides the conclusions of our paper.

II. Problem Formulation

A. Overview of CRAS

In this work, we have considered a combined event and parameter-based CRAS, as shown in Fig. 1, where the CRAS

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2021.3066316, IEEE Transactions on Smart Grid

controller (CRASc), operating at the control center, receives phasor measurements of critical lines and generators from different substation zones through synchrophasor network and later performs corrective actions like generation shedding, as defined in the North American Electric Reliability Corporation (NERC) guideline [34], by sending control signals through the SCADA communication. The complete operation of CRAS is divided into four major steps.

Step 1: The CRASc, initially at an armed stage, collects phasor data at a regular interval in terms of relays status, power line flows, and generator power output of substation zones.

Step 2: The CRASc gets triggered during a line outage and checks the operational transfer capability (OTC) limit of other critical adjacent lines in that substation zone.

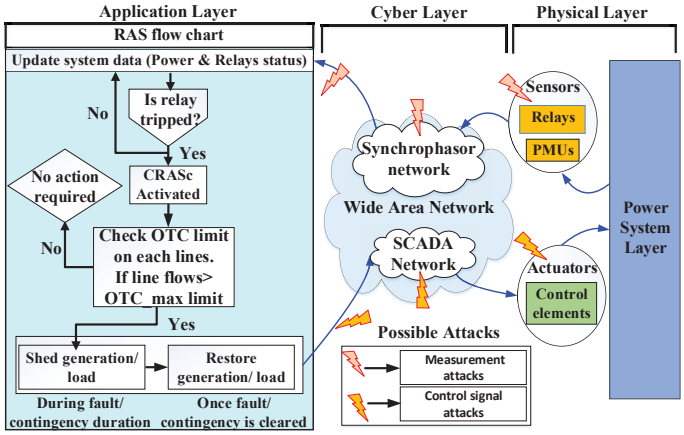


Fig. 1: Flowchart of CRAS and its cyberattack surface

Step 3: If current line flows exceed their maximum operational transfer capability (OTC_max) limits, the CRASc curtails the generation to prevent the thermal overloading in other adjacent critical lines. Note that the thermal overload limit is considered while computing the OTC_max limits, which is provided through a predefined action table based on offline contingency analysis of substation zones.

Step 4: Also, the CRASc restores the generation once a fault or line contingency is cleared [34].

B. Cyber and Physical Events

1) Cyber Events

Based on possible attack surfaces on measurement and control signals, as highlighted by lightning bolt symbols in Fig. 1, we have considered following types of cyberattacks.

a) ***Generation altering attack***: Modification of a control signal to unnecessarily alter the generation. In particular, we have considered two attack templates: pulse and ramp attacks [17], to perform this attack.

Pulse attack: It involves periodically changing an input control signal by adding the pulse attack parameter, λ_{pulse}, for a small time interval, (t_1). It retains the original input for a remaining interval, $(T - t_1)$, for the given time period, (T), as shown in (1).

Ramp attack: It involves adding a time-varying ramp signal to the input control signal based on a ramp signal parameter, λ_{ramp}, as shown in (2).

$$P_{pulse} = \begin{cases} P_i(1 + \lambda_{pulse})(t = t_1) \\ P_i(t = T - t_1) \end{cases} \quad (1)$$

$$P_{ramp} = P_i + \lambda_{ramp} * t \quad (2)$$

b) ***Malicious tripping attack***: Unauthorized tripping of a relay, also known as an intelligent electronic device (IED), by launching a trip command using SCADA protocols to disconnect the transmission line.

c) ***False-data-injection (FDI) attack***: Injecting malicious phasor measurements, disguised as genuine measurements, by successfully conducting a man-in-the-middle (MITM) attack over the network to provide an incorrect situational awareness to the CRASc.

d) ***Denial of Service (DoS) attack***: Performing a SYN flood attack by repeatedly sending the SYN packets on the targeted substation-based data aggregator to disrupt the synchrophasor communication between substation and control center.

e) ***Coordinated cyberattack***: Combination of attack vectors on measurement and control signals where deceptive phasor measurement signals are injected before modifying control signals to nullify the operation of CRASc. In this category, three attacks are considered: 1) FDI attack followed by a malicious tripping attack, 2) FDI attack followed by a pulse attack, 3) FDI attack followed by a ramp attack.

2) Physical Events

Apart from cyberattacks, we have also considered several natural/man-made line faults at the power system layer. It includes symmetrical and asymmetrical line faults that can happen on transmission lines.

C. Assumptions

The smart grid consists of several substations that rely on several legacy devices and SCADA and synchrophasor communication protocols to facilitate the CRAS operation. Since these communication protocols, including Distributed Network Protocol (DNP3), IEC 61850, IEEE C37.118, etc. are generally not encrypted, there are numerous possible ways of performing cyberattacks despite the existing defense mechanisms, such as firewall, virtual private network (VPN), and NERC Critical Infrastructure Protection (CIP) standards. Further, the substation-based remote terminal units (RTUs) and local phasor data concentrators (PDCs) are mostly embedded devices and do not provide enough computational power and functionality to support authentication and protocol encryption. The National Electric Sector Cybersecurity Organization Resource (NESCOR) group [35] discussed the existing vulnerabilities in communication protocols and devices in the WAMPAC cybersecurity. From a real-world perspective, it is extremely difficult for an attacker to get unauthorized access to several substation zones at the same time when these zones are geographically dispersed; and are operating in a secure environment. From the attack side, we assume that the attacker has access to one of the substation zones; and can compromise and manipulate measurement or control signals for that specific zone to perform single and coordinated cyberattacks.

D. Problem Statement

The main goal of this research is to develop a real-time CPADS for the CRAS by utilizing data-driven algorithms, PMU measurements, and cyber properties (network packets)

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2021.3066316, IEEE Transactions on Smart Grid

to detect anomalies and provide a detailed classification of cyberattacks and power system disturbances. In this work, different classes of attacks are considered to develop a robust and efficient CPADS. Based on the stated assumptions and the existing attack surfaces, the proposed algorithm should be able to achieve a high detection accuracy with acceptable latency bounds while supporting scalability to large grid networks and applying to a wide range of CRAS configurations. Further, the proposed CPADS will assist in developing effective mitigation strategies tailored to these events to restore the normal grid operation after disturbances.

III. Proposed Architecture and Methodology

A. Proposed Architecture

Fig. 2 shows the proposed architecture of CPADS for the CRAS that consists of multiple anomaly detectors (Anomaly detector A...Anomaly Detector N) that are operating at the secure control center. To facilitate the accurate and reliable operations of CRAS, the whole power system is divided into several substation zones as Zone A...Zone N. For different buses in the interconnected grid, system dynamics and magnitude of disturbances could be very different and a *"one size fits all"* solution is not suitable for accurately detecting attacks. Therefore, we are proposing multiple anomaly detectors-based CPADS, where an individual anomaly detector is dedicated to the specific substation zone that oversees a few critical substations and detects possible cyber intrusions in that zone. Note that the operation of each anomaly detector is not dependent on other anomaly detectors for detecting attacks in the assigned zone, and it eventually assists CRASc in taking appropriate corrective actions. Further, the proposed architecture receives three different types of data sources as an input data that are discussed here.

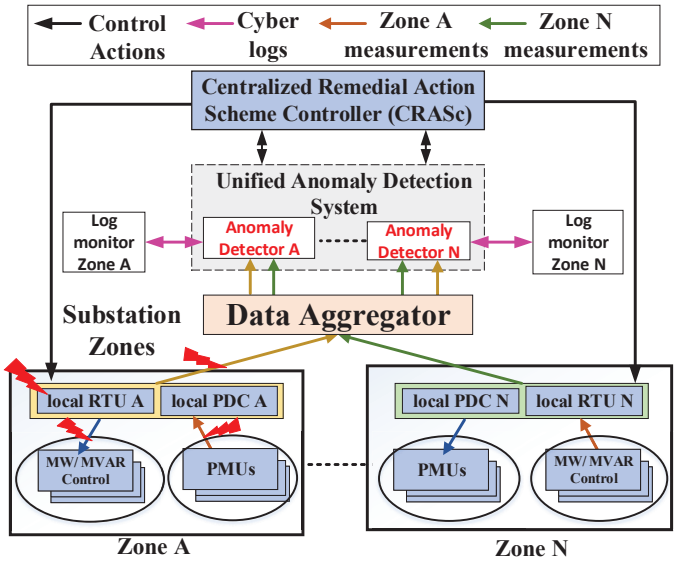


Fig. 2: Proposed architecture of CPADS with CRAS

1) Input data

While assuming total substation zones N, the proposed anomaly detector (i.e. anomaly detector A), operating for the substation zone A, receives raw input data as time-stamped N_s samples of PMU data points X_a that consists of a set of local PMU measurements X_{la}, PMU network properties C_{la}, and redundant PMU measurements X_{ra} from the remaining N-A substation zones, as shown in (3).

$$X_a = [\underbrace{X_{la}}_{Local}, \overbrace{C_{la}}^{Cyber}, \underbrace{X_{ra}}_{Redundant}] \tag{3}$$

$$X_{la} = [Vg_a, Fg_a, (V_{1a}, V_{2a}, V_{0a})_i, (V_{1a}, V_{2a}, V_{0a})_j] \tag{4}$$

$$C_{la} = [s_{ka}, t_{ka}] \tag{5}$$

a) **Local PMU measurements** (X_{la}): Consist of a positive sequence generation bus voltage (Vg_a), generator frequency (Fg_a), and positive, negative, and zero sequence components ($(V_{1a}, V_{2a}, V_{0a})_i$, $(V_{1a}, V_{2a}, V_{0a})_j$) of bus voltages at sending and receiving ends of critical transmission lines, as denoted by subscripts i and j in (4). These measurements are collected from deployed PMUs in the substation zone A during a regular operation of CRAS.

b) **PMU Network Properties** (C_{la}): Include packet size s_{ka} with a timestamp t_{ka} of incoming synchrophasor network packets from the substation zone A at the instant (k), as represented in (5).

c) **Redundant PMU measurements** (X_{ra}): Consist of a same category of PMU measurements ((X_{ra}) of other substation zones N-a that are forwarded to the anomaly detector A through the control center-based data aggregator.

Note that the proposed multi-source input data is based on the notion that the injected disturbances at one node are propagated to other adjacent and connected nodes in a well-coordinated way that can be utilized for detecting different classes of cyberattacks.

B. Proposed Methodology

Fig. 3 illustrates the proposed methodology of each anomaly detector (i.e. anomaly detector A) that receives X_a to perform multi-events classification using three classification models: model 1 (M1), model 2 (M2), and model 3 (M3). These three classifiers receive different sets of input features, as shown in Fig. 3, and the output of these classifiers are utilized to perform final events identification using a rules-based decision logic. The mechanism for developing this methodology consists of three phases: 1) offline process for developing, training, and updating classification models with new scenarios or cases when models are not online, 2) online process for computing and extracting relevant features, and testing classification models, and 3) rules-based decision logic for final events identification.

1) Offline Process

The offline process, common for all three classification models, consists of three different modules that are elaborated in greater detail below.

Step 1 (Labeled dataset generation module): In this module, a library of the training dataset is generated through a HIL real-time simulation of several cyber-physical scenarios, including cyberattacks and line faults while assigning class labels. The modeled system is characterized by generators capacity, load levels, system topology, etc., to generate a library of training datasets $L_m = (U, V)_m$ of L samples for a classification

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2021.3066316, IEEE Transactions on Smart Grid

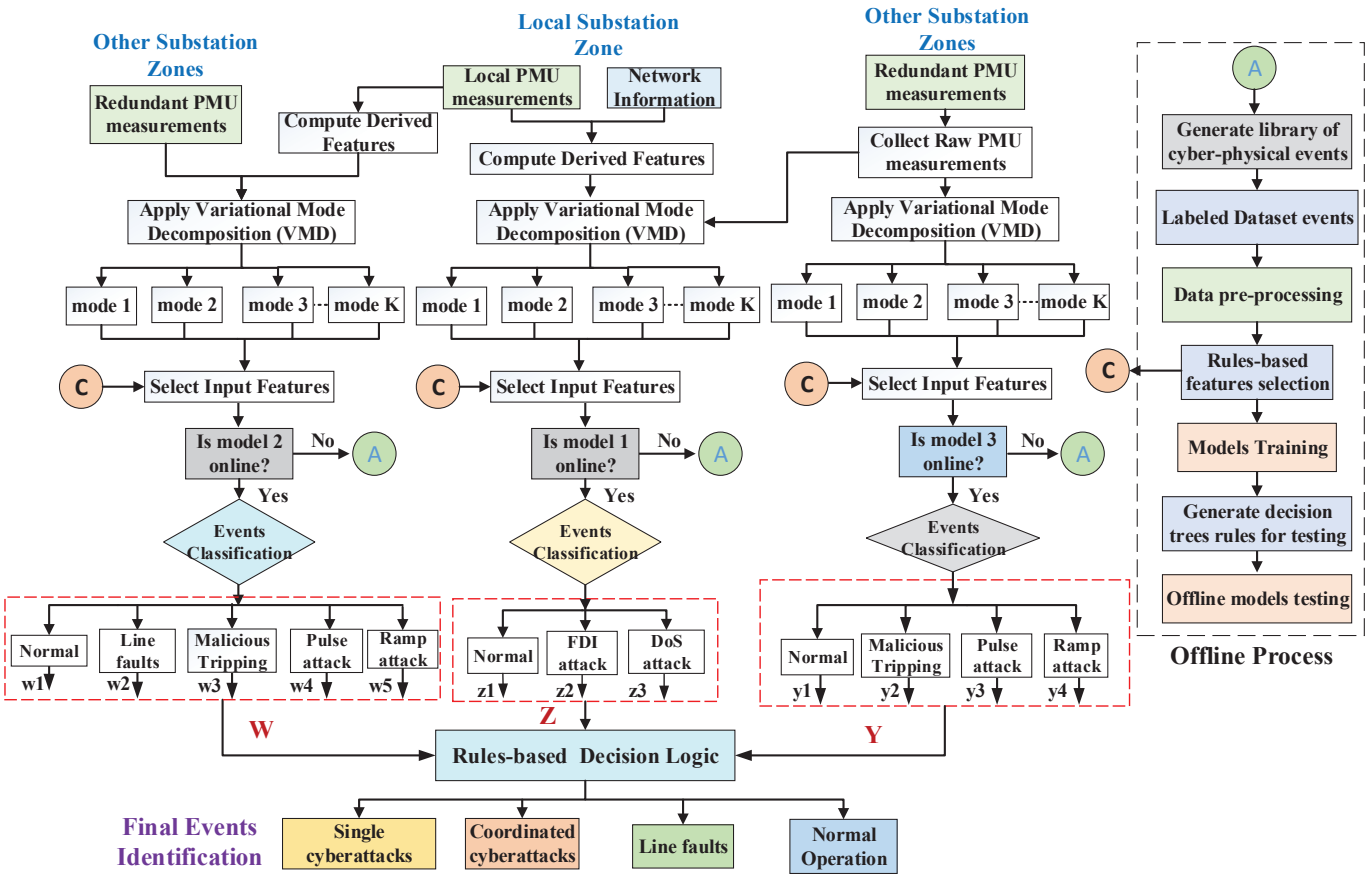


Fig. 3: Proposed methodology of an anomaly detector

model m, where U=$[f_1, f_2, ...f_p]$ is a set of p features and V is a set of labels corresponding to U.

Step 2 (Data pre-processing module): This module includes data cleaning, normalization, and rules-based features selection to eliminate weakly and irrelevant features that may affect the performance of classification models.

a) **Data cleaning and normalization**: Data cleaning provides quality assessment by filtering inconsistent values and eliminating rows with missing data. Data normalization scales L_m to a normalized dataset L'_m such that samples of each input feature $f_i[j]_{j=1}^{Z}$ $i \in \{1, P\}$ lie in the range [0 1], which enhances smoothness and improves homogeneity among samples.

b) **Rules-based features selection**: Selection of optimal features requires an expert knowledge and detailed investigation of L'_m. Based on the nature of classification models, a combination of filter and wrapper-based feature selection approaches is proposed to obtain necessary features. In particular, best first search (BFS) algorithm, one of the wrapper methods, is utilized to select relevant features from U that are weakly correlated among them and strongly correlated to V in a forward selection process [35]. Also, Pearson's correlation coefficient (P_c) technique, one of the filter methods, is applied to quantify the degree of correlation among features in U. For a given two input features f_i and f_j ($[f_i, f_j] \in$U), it is computed using (6) where $cov(f_i, f_j)$ is the covariance, $var(f_i)$ and $var(f_j)$ are variances of f_i and f_j.

$$P_c(f_i, f_j) = \frac{cov(f_i, f_j)}{\sqrt{var(f_i)var(f_j)}} \tag{6}$$

In particular, we have defined two rules to select relevant features for M1, M2, and M3 that are explained for the anomaly detector A.

Rule 1: For M1 that receives X_a category of input data, the relevant features are selected in two stages. The first stage involves separately selecting independent and weakly correlated features in intra-substation zone measurements, which are substation zone A measurements ($[X_{la}, C_{la}]$) and X_{ra} from N-A substation zones, by applying the BFS algorithm. In the second stage, the previously selected features of X_{la} and X_{ra} are again filtered by applying P_c for selecting final features that exhibit medium to high inter-substation zones correlation ($\pm$0.75 to $\pm$ 1) between the selected features of substation zone A and substation zones N-A. This two-stage selection process is based on the notion that the electrically-close PMU measurements from N-A substation zones can be utilized to detect FDI attacks on local measurements of substation zone A.

Rule 2: For M2 and M3, the BFS algorithm is applied to select independent features in U that are weakly correlated among them while exhibiting a high correlation to V.

Step 3 (Training module): In this module, the obtained datasets L''_m of previously selected features are used as inputs for training a random decision tree (DT)-based classifiers in M1, M2, and M3. The DT generates a tree-like structure by

repeatedly splitting L''_m into small and optimal subsets until each partition contains only samples of one class label. The generated decision tree rules after training of M1, M2, and M3 are applied later for online testing during event classifications.

2) Online Process

This process consists of computing derived features, VMD-based features extraction and normalization, testing trained classification models, and applying rules-based decision logic for identifying events.

Step 1 (Derived features computation): From the power system's perspective, the injected transient disturbances during data integrity (cyber) attacks and natural/man-made physical events, such as line-faults may look similar; however, these events leave a unique signature on raw PMU measurements that can be extracted by computing derived features (attributes). Therefore, we have computed derived features ([X_{la}', C_{la}']) from local measurements ([X_{la}, C_{la}]) where $X_{l'a}$=[$|X_{la}|^2, \Delta X_{la}, \frac{dX_{la}}{dt}$] is computed from X_{la}, as shown in (7) to (9). $|X_{la}|^2$ is a square of phasors magnitude, ΔX_{la} includes a change in generator bus voltage ΔVg_a and frequency ΔFg_a, and difference in symmetrical components of sending and receiving ends of line voltage $\Delta[V_{1a}, V_{2a}, V_{0a}]_{ij}$, and $\frac{dX_{la}}{dt}$ are their respective derivatives.

$$|X_{la}|^2 = [|Vg_a|^2, |Fg_a|^2, [|V_{120a}|]_i^2, [|V_{120a}|]_j^2] \quad (7)$$

$$\Delta X_{la} = [\Delta Vg_a, \Delta Fg_a, \Delta[V_{1a}, V_{2a}, V_{0a}]_{ij}] \quad (8)$$

$$\frac{dX_{la}}{dt} = \left[\frac{dVg_a}{dt}, \frac{dFg_a}{dt}, \frac{[dV_{1a}, dV_{2a}, dV_{0a}]_{ij}}{dt}\right] \quad (9)$$

From C_{la}, four features are computed using (10) to (12) where the first two features of $C_{l'a}$ include moving average (M(Δs_{ka}), M(Δt_{ka})) of change in packet size (Δs_{ka}) and timing difference between two consecutive packets (Δt_{ka}) and the remaining two features are their standard deviations (S(Δs_{ka}),S(Δt_{ka})). A sliding window l=10 is considered while computing these features.

$$C_{l'a} = [M(\Delta s_{ka}), M(\Delta t_{ka}), S(\Delta s_{ka}), S(\Delta t_{ka})] \quad (10)$$

$$M(x) = \frac{1}{l}(\sum_{i=1}^{l} x_i) \quad (11)$$

$$S(x) = \sqrt{\frac{1}{l-1}\sum_{i=1}^{l} |x_i - M(x)|^2} \quad (12)$$

Step 2 (VMD-based features extraction): The VMD technique is applied to extract distinctive features by decomposing a multi-component signal $u(t)$ into a set of sub-signal modes $u_k(t)$, also known as band-limited intrinsic mode functions (IMFs) with the specific sparsity properties [31]. The resulting constrained problem of the VMD algorithm is formulated as

$$\min_{(\{u_k\},\{w_k\})} \left\{ \sum_{k=1}^{K} \left\| \partial_t \left[(\delta(t) + \frac{j}{\pi t}) \times u_k(t) \right] e^{-jw_k t} \right\|_2^2 \right\} \quad (13)$$

subject to $\sum_{k=1}^{K} u_k = f$

where w_k is the estimated center frequency around which the k^{th} decomposed mode u_k is mostly compact. A vmd function is defined to calculate K decomposed modes, $\{mode1, mode2...modeK\}$=$\{u_1 \dots u_K\}$ from N_s samples as

$$\{u_1, u_2, ..u_K\} = vmd(u(t), \alpha, K, Tol) \quad (14)$$

where α is a bandwidth constraint, $u(t) \in$ ($X_{l'a}$, X_{ra}), K is a mode count, and Tol is a convergence tolerance level.

In this work, α is set to a lower value (α=200) to capture a wide range of frequency contents in $u(t)$. Since K decides the total decomposed modes, its value is assigned to 4 (K=4), similar to the total labeled classes in each model, and Tol=10^{-7}. The computed modes U_{la} from $X_{l'a}$ and U_{ra} from X_{ra} with $C_{l'a}$ are utilized later for generating a library of labeled datasets ($U \in$ [U_{la}, U_{ra}, $C_{l'a}$]), applying rules-based features selection, and training and building classification models through the offline process as discussed earlier.

The overall detection algorithm is summarized here.

Algorithm 1: Proposed Anomaly Detection Algorithm

Input: X_{la}, C_{la}, X_{ra}
Output: O
Parameters: l, K, Tol, α, m;
Initialization: set l=10, K=4, α=200, Tol=10^{-7},m=0
while $t \geq t_o$ **do**
  Compute $X_{l'a}$ from X_{la} and $C_{l'a}$ from C_{la}
  Apply vmd and compute U_{la} & U_{ra}
  m=m+1
  if m=*1* **then**
    Generate L_1 datasets & compute L'_1 & L''_1
    Train VMD-DT1(U_{la}, U_{ra}, $C_{l'a}$) using L''_1
    Output events Z ($z1$, $z2$, $z3$)
  else if m=*2* **then**
    Generate L_2 datasets & compute L'_2 & L''_2
    Train VMD-DT2(U_{la}, U_{ra}) using L''_2
    Output events W ($w1$, $w2$, $w3$, $w4$, $w5$)
  else if m=*3* **then**
    Generate L_3 datasets & compute L'_3 & L''_3
    Train VMD-DT3(U_{ra}) using L''_3
    Output events Y ($y1$, $y2$, $y3$, $y4$)
  while Z=$z1$ **do**
    O=W; Output events to the CRASc
  else if $Z \neq z1$ **then**
    O=Y; Output events to the CRASc

Step 3 (Classification models testing): In this process, three supervised classification models: M1, M2, and M3 perform independent predictions of events as discussed here.

M1 anomaly detector: This model VMD-DT1(U_{la}, U_{ra}, $C_{l'a}$) receives U_{la}, U_{ra}, and $C_{l'a}$ categories of measurements, selects relevant features from L'_1 using rule 1, performs offline training using L''_1 datasets, and returns a set of class labels Z ($z1$, $z2$, $z3$), where $z1$ represents a normal event, $z2$ and $z3$ are FDI and DoS attacks.

M2 anomaly detector: This model VMD-DT2(U_{la}, U_{ra}) receives U_{la} and U_{ra} categories of measurements, selects relevant features from L'_2 using rule 2, performs offline training using L''_2 datasets, and returns a set of class labels W

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2021.3066316, IEEE Transactions on Smart Grid

($w1$, $w2$, $w3$, $w4$, $w5$), where $w1$ represents a normal event, $w2$ represents line faults, $w3$ represents a malicious tripping attack, $w4$ and $w5$ are pulse and ramp attacks.

M3 anomaly detector: This model VMD-DT3(U_{ra}) receives only U_{ra} category of measurements, selects relevant features from L_3' using rule 2, performs offline training using L_3'' datasets, and returns a set of class labels Y ($y1$, $y2$, $y3$, $y4$), where $y1$ is a normal event, $y2$ represents a malicious tripping attack, $y3$ and $y4$ are pulse and ramp attacks.

3) Rules-based Decision Logic

This final phase receives class labels Z, W, and Y from M1, M2, and M3 and provides final cyber-physical events classification O, including normal operation, line faults, single, and coordinated cyberattacks based on the defined two rules-based logic.

Rule 1: If Z = $z1$ (normal event) in M1, then W of M2 is forwarded to the CRASc (i.e. O=W), and Y of M3 is discarded to detect faults and single cyberattacks using M1 accurately.

Rule 2: If Z = $z2$ or $z3$ in M1, then Y of M3 is forwarded to the CRASc (i.e. O=Y) and W is discarded as the X_{la} of substation zone A are either compromised or unavailable due to FDI or DoS attacks, and coordinated cyberattacks are detected using M1 and M3 accurately.

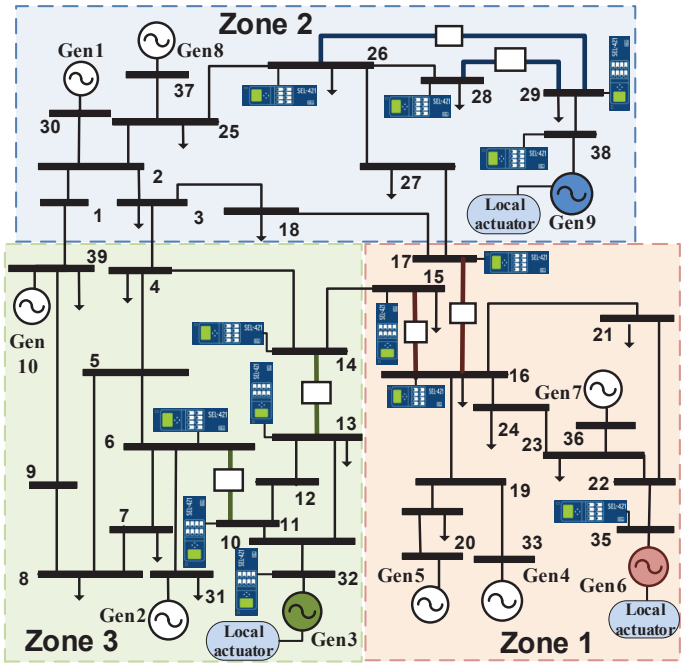


Fig. 4: IEEE 39 bus with PMU-based CRAS

IV. Experimental Evaluation

A. System Topology and Experimental Setup

Fig. 4 shows the modified IEEE 39 system that is divided into three major zones: zone 1, zone 2, and zone 3. Based on the offline contingency analysis, we have deployed a CRASc to prevent the thermal overload during single-line outages in different zones. For zone 1 operation, the CRASc receives PMU data of line buses 15, 16, and 17, and generator bus 35, to monitor disturbances, especially a single line outage. During the tripping of line L16-17, the CRASc is activated and sheds the generation at bus 35 to maintain the power flow limits and prevent overloading in line L15-16. In addition, the CRASc also receives phasor measurements of line buses 26, 28, and 29 and generator bus 38 for the zone 2; and line buses 11, 6, 13, and 14 and generator bus 32 for the zone 3, to detect disturbances and provide an appropriate generation shedding in their respective zones.

TABLE I: Datasets for training and testing models

Scenarios			Cases
Physical Disturbances			
Line faults	**Fault Location**	**Fault Duration**	
Asymmetrical L-G(A-G), LL-G (AB-G), L-L (A-B)	0.3, 0.5, 0.7	4.8, 6, 7.2	270
Symmetrical L-L-L (A-B-C), LLL-G (ABC-G)	0.3, 0.5, 0.7	4.8, 6. 7.2	180
Single cyberattacks			
Malicious Tripping	Line = L16-17		10
Pulse Attacks	Duty=[0.3, 0.5, 0.8], Period=[-2, -2.5, -3, -3.5]		120
Ramp Attacks	Ramping Steps/sec = [2, 3, 4, 5]		40
Denial of Service (DoS) Attack	[(Packet numbers, Packet size)] = [(3000,350), (4000,450)...(11000, 1150)]		90
Coordinated cyberattacks			
MITM (FDI) + Malicious Tripping	Line = L16-17		10
MITM (FDI) + Pulse Attacks	Duty=[0.3, 0.5, 0.8], Period=[2, 2.5, 3, 3.5]		120
MITM (FDI) + Ramp Attacks	Steps = [2, 3, 4, 5]		40

To validate the proposed approach, the anomaly detector for zone 1 (i.e. anomaly detector 1) is tested and evaluated in the HIL cyber-physical testbed environment, as shown in Fig. 5. The selected IEEE 39 bus system is modeled in ARTEMiS-SSN (State-Space Nodal) solver in eMEGASIM (RT-Lab) environment and simulated using OP5600 OPAL-RT real-time digital simulator at a smaller time step of 50 μs. The simulator is mapped to two physical (SEL-421) relays through the IEC 61850-8-1 GOOSE communication message to enable circuit breakers for lines L15-16 and L16-17, as relay 1 and relay 2. Further the modeled virtual PMUs, inside the simulator, are sending phasor measurements at a sampling rate of 60 frames/second to two SEL-3573 local PDCs, where LPDC1 operates as a local PDC for the substation zone 1 and LPDC23 operates as a local PDC for the substation zone 2 and zone 3. The control center-based central PDC (OpenPDC) receives data from local PDCs and stores it in a historian comma-separated values (CSV) files and MySQL database. We have utilized the Wireshark tool, an open-source network analyzer, to monitor network traffic and store network logs in the CSV files. The CRASc periodically polls the data from the MySQL database in real-time, and provides necessary SCADA-based control signals to the simulator through a substation RTU using the Kepserver's OPC Unified Architecture (UA) client-server interface to close the loop. For developing classification models using the stored CSV files, we have applied the WEKA, an open-source machine learning platform, which supports several supervised machine learning algorithms that can be utilized for developing classifiers.

B. Labeled Datasets Preparation

Table I presents a list of several cases with different scenarios that we have considered for generating datasets through the tesbed-based experiments. While simulating physical line faults, we have considered asymmetrical and symmetrical line faults on Line L16-17 for three fault locations (0.3, 0.5 and 0.7 p.u.) and three fault durations (4.8, 6, 7.2 cycles) followed by the normal tripping of line for different operating points.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2021.3066316, IEEE Transactions on Smart Grid

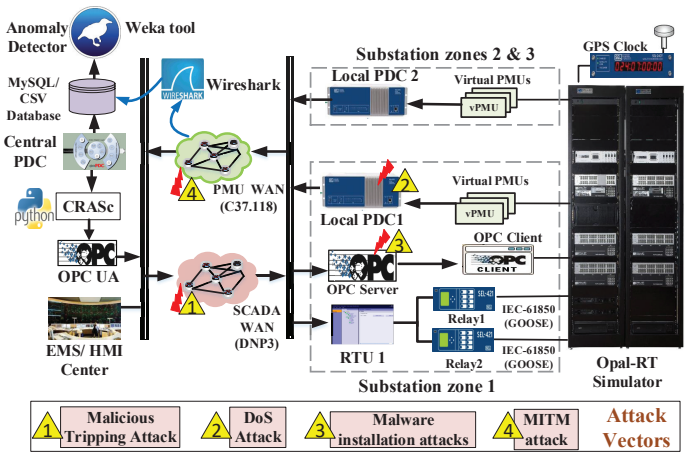


Fig. 5: HIL experimental setup for attack-detection experiment

Note that we have varied the generation at bus 35 from 610 MW to 700 MW and the load at bus 18 from 118 MW to 208 MW in a step increase of 10 MW to create 10 operating points while maintaining the generation-load balance.

For performing single cyberattacks in zone 1, we have considered four attacks; malicious tripping, pulse, ramp, and DoS attacks, at different operating points. During the malicious tripping attack, a single line outage (L16-17) is considered for different operating points. During pulse attack, we have considered three duty cycles (t_1/T = [0.3, 0.5, 0.8]) and four time periods (T = [2, 2.5, 3, 3.5]) with λ_{pulse} = -0.8. In case of ramp attack, four negative ramping steps/sec, λ_{ramp} = [-2, -3, -4, -5], are considered to gradually reduce the generation at bus 35 for different operating points. During the SYN flooding-based DoS attack, packets number and size are varied from (3000, 350) to (11000, 1150) in a step increase of 1000 packet numbers and 100 packet size to create 90 cases.

During the coordinated cyberattacks, we have considered three attack vectors, where a MITM attack is performed on phasor measurement signals of the zone 1 followed by attacks, including malicious tripping, ramp, and pulse attacks, on control signals for the same number of scenarios, as mentioned in the single cyberattacks. In total, we have considered 880 cases of cyber-physical events; where 450 cases are simulated line faults, 260 are single attacks, and the remaining 170 cases represent coordinated cyberattacks.

C. Testbed-based Implementation

Fig. 5 also presents the experimental setup for implementing cyberattacks and generating heterogeneous datasets, as necessary for training and testing classification models. The malicious tripping attack is performed on the relay 2 by replaying the tripping packet, captured during the normal tripping operation, using a python script between the substation and control center, as shown by yellow triangular box 1. The DoS attack is performed to break the synchrophasor communication between LPDC1 and OpenPDC, as shown by yellow triangular box 2. It is implemented by sending a huge number of random packets to the LPDC1 through the TCP SYN flooding attack using hping tool, available in the Kali Linux machine. For deploying generation altering attacks, including ramp and pulse attacks, on the generator 35 (G35), the malware installation-based attack is performed by installing the malware, Trojan Horse, on the OPC server-based substation RTU, as shown by yellow triangular box 3. The installed malware provides a backdoor access to close the legitimate RTU program and initiate python script-based malicious logic that periodically sends malicious control signal to initiate ramp and pulse attacks on the generator (G35).

To perform coordinated cyberattacks, we have performed a Man-in-the-Middle (MITM) attack, as a FDI attack vector, between the LPDC1 and control center-based OpenPDC, as shown by yellow triangular box 4, followed by malicious tripping, ramp, and pulse attacks. For performing the MITM attack, an address resolution protocol (ARP) spoofing attack is implemented using a Kali Linux machine to poison the ARP cache table. Later, the Linux-based PMU simulator tool, PMUSim, masquerading as a legitimate PMU, sends malicious phasor measurements to the OpenPDC [36]. The malicious PMU measurements include replaying last 60 samples of PMU data captured during the normal operation using the Wireshark. For simulating physical disturbances, including symmetrical and asymmetrical line faults, we have utilized the Python-based application programming interface (API) of the simulator to perform automated and multiple simulations for different operating points.

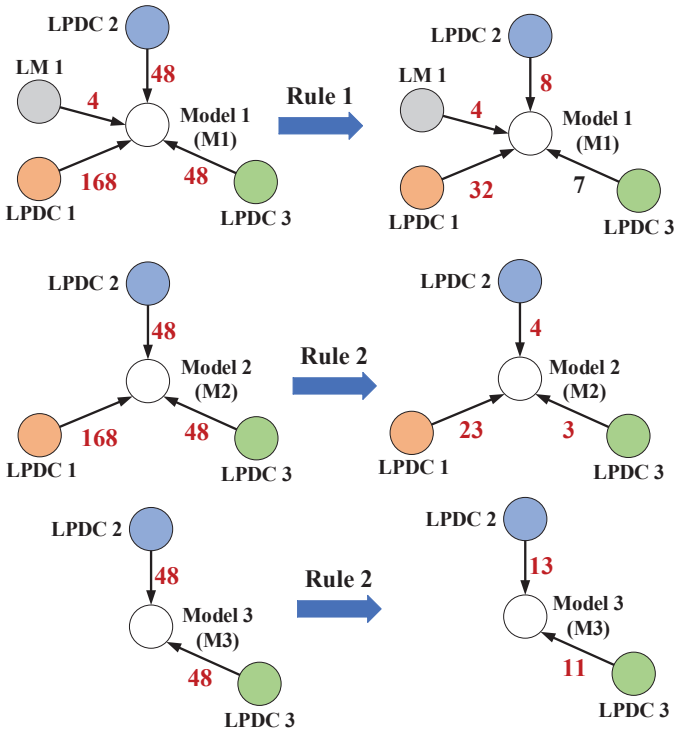


Fig. 6: Rules-based features selection for classification models (M1, M2, & M3) for an anomaly detector 1

D. Features Extraction and Training Models

During the offline process, several relevant features are selected by applying the proposed rules-based features selection approach for classification models M1, M2, & M3 of the anomaly detector 1. Fig. 6 illustrates this selection approach using the *ball-and-stick diagram* where colored balls (orange, sky blue, and green) represent the local PDCs of zone 1, zone

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2021.3066316, IEEE Transactions on Smart Grid

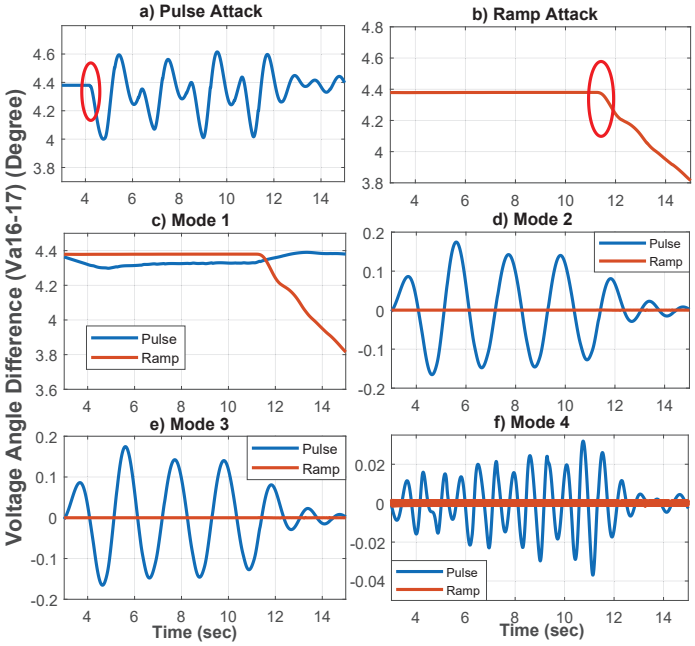


Fig. 7: VMD application for features extraction

2, and zone 3, a grey colored ball shows the log monitor (LM 1) of zone 1, and arrow illustrates the total number of features that are received by classification models before and after the selection process. These classification models are represented by non-colored balls in Fig. 6. Initially, 268 features for M1, 264 features for M2, and 96 features for M3 are considered for the classification process; however, after applying the rules-based features selection process, 51 features for M1, 30 features for M2, and 24 features for M3 actually participate in training these models. Further, the proposed selection technique is investigated for classification accuracy that reveals an increment in an accurate rate of 0.4%, 0.04%, and 0.45% in M1, M2, and M3. Note that while training these models, the selected system was simulated for 5 seconds to capture the system dynamics for each scenario that corresponds to 300 samples (60 samples/second) per scenario. These 300 samples of data were selected from a time instant when an event has initiated. Once the heterogeneous database is generated, 70% of the data is utilized for training models and the remaining 30% is utilized for testing models. Since we are interested in characterizing different events based on the deviation from the nominal value in a small-time frame, irrespective of the shape of a signal curve, we process the obtained VMD-based decomposed modes at each time step independent from the previous time step, and feed into the decision tree-based models to perform multi-classification.

E. VMD Application on Time-Series Data

Fig. 7 presents an illustrative example that walks through the application of VMD algorithm to validate its effectiveness in extracting features for detecting anomalies. For a sample case study, the positive sequence voltage angle difference (Va16-17) between the bus 16 and bus 17 of IEEE 39 bus system, one of the selected derived features, is decomposed into four modes with different frequencies using VMD technique. Fig. 7 (a) and Fig. 7 (b) represent original input signals during pulse and ramp attacks on generator 35. During the pulse attack, the low-frequency transient is extracted in the first mode (mode 1) that provides the rough estimation of states, and medium and high (impulsive) frequency components are separately extracted in the second (mode 2), third (mode 3), and forth mode (mode 4). Since ramp attack gradually changes system dynamics, the first mode effectively estimates the input signal. In contrast, the computed medium and higher modes in ramp attack do not exhibit any frequency oscillation as compared to pulse attack. The above observations signify the efficiency of the VMD technique to locate system states and capture the high-order non-sinusoidal spikes in transient signals.

V. Results and Discussions

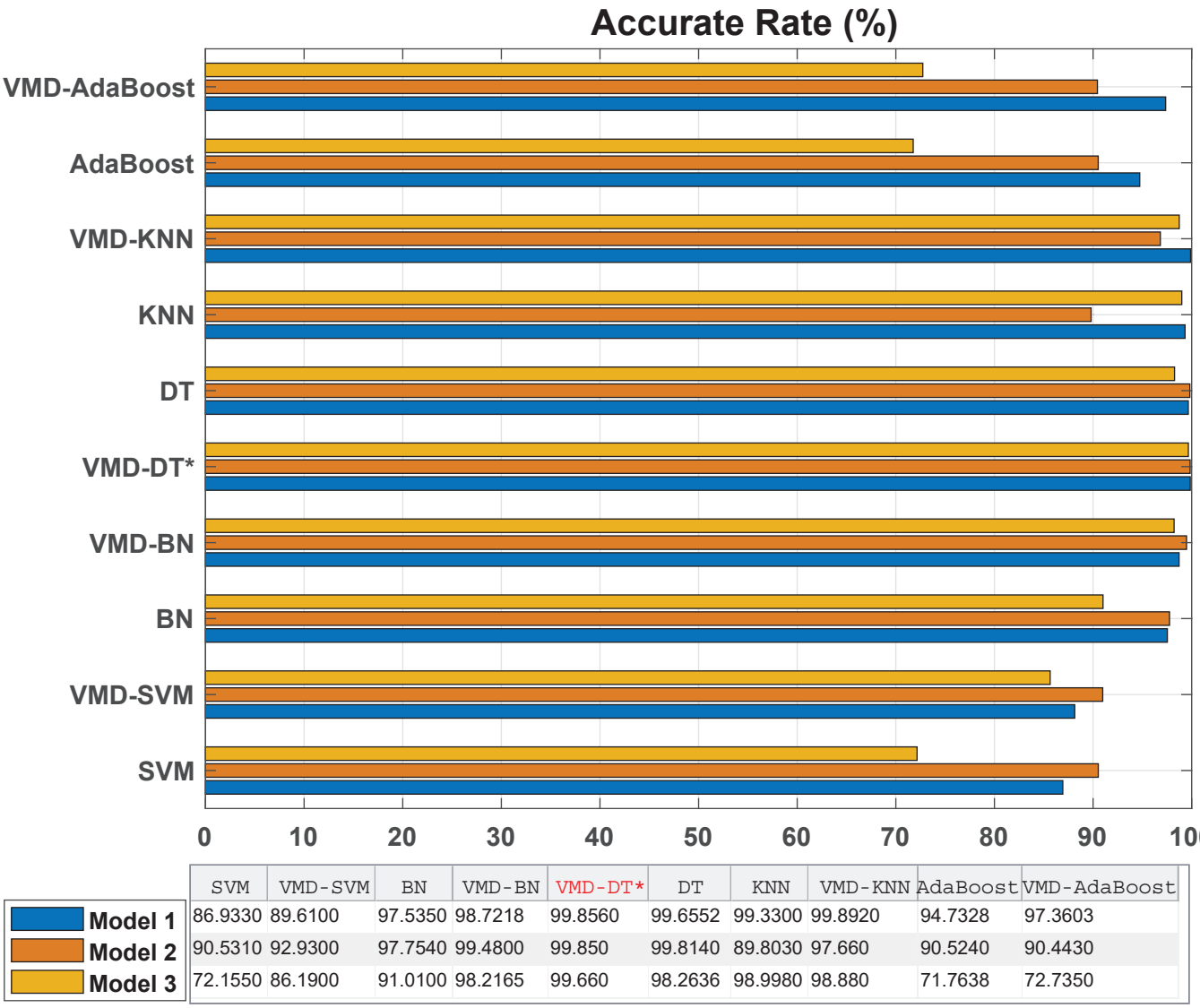
Since the false prediction of events would mislead the CRASc to take inappropriate actions, we have considered several performance measures to evaluate the proposed anomaly detector 1 of CPADS. Fig. 8 shows the accuracy rate (%) of several machine learning algorithms, such as support vector machine (SVM), DT, bayesian network (BN), k-nearest neighbors (KNN), AdaBoost, and VMD-applied algorithms (VMD-SVM, VMD-BN, VMD-DT, VMD-KNN, and VMD-AdaBoost) for M1, M2, and M3 classifiers. Note that we have tuned the parameters of these machine learning algorithms to optimize their performances using the 10-fold cross validation. It can be observed that the proposed VMD-DT algorithm exhibits superior performance with an accuracy rate of 99.856% for M1, 99.85% for M2, and 99.66% for M3 as compared to other classifiers. Besides, Fig. 8 presents the significance of VMD technique as the accuracy of other VMD applied algorithms has improved at a certain level in most of the cases. Apart from the accuracy rate, we have also considered other performance measures, namely average recall, average precision, and average F-measure to validate the performance of classifiers. Recall, also known as sensitivity, defines the true positive rate (TPR), precision measures the positive predictive value, and F-measure, which provides a balance between the precision and recall, is calculated based on recall and precision. These performance measures are calculated using (15) to (17) where TP_i, FN_i, and FP_i are true positives, false negatives, and false positives of i^{th} class and K is the total number of classes. Table II presents a comparison of VMD-DT with a decision tree (DT) algorithm, where the proposed VMD-DT algorithm shows a consistent and better performance for all three models as compared to the DT algorithm with same datasets.

$$\text{Average Recall (AR)} = 1/K \sum_{i=1}^{K} \frac{TP_i}{TP_i + FN_i} \tag{15}$$

$$\text{Average Precision (AP)} = 1/K \sum_{i=1}^{K} \frac{TP_i}{TP_i + FP_i} \tag{16}$$

$$\text{Average F-measure (AF)} = 1/K \sum_{i=1} 2.\frac{P_i.R_i}{P_i + R_i} \tag{17}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2021.3066316, IEEE Transactions on Smart Grid



SVM	VMD-SVM	BN	VMD-BN	VMD-DT*	DT	KNN	VMD-KNN	AdaBoost	VMD-AdaBoost
86.9330	89.6100	97.5350	98.7218	99.8560	99.6552	99.3300	99.8920	94.7328	97.3603
90.5310	92.9300	97.7540	99.4800	99.850	99.8140	89.8030	97.660	90.5240	90.4430
72.1550	86.1900	91.0100	98.2165	99.660	98.2636	98.9980	98.880	71.7638	72.7350

Fig. 8: Accuracy plot of classifiers for M1, M2, and M3

TABLE II: Performance metrics for different classifiers

Parameters	VMD-DT	DT
Model 1 (M1) Performance		
Average Recall	0.986	0.982
Average Precision	0.989	0.983
Average F-Measure	0.988	0.982
Model 2 (M2) Performance		
Average Recall	0.995	0.991
Average Precision	0.995	0.993
Average F-Measure	0.995	0.992
Model 3 (M3) Performance		
Average Recall	0.997	0.984
Average Precision	0.997	0.985
Average F-measure	0.997	0.984

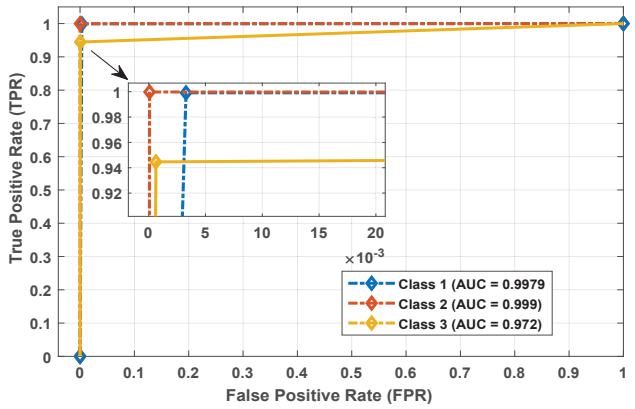
TABLE III: Performance metrics during the stratified k-fold cross validation

Parameters	Model 1	Model 2	Model 3
Accuracy (%)	99.8572	99.8773	99.6206
Average Recall	0.9813	0.9962	0.99625
Average Precision	0.9826	0.9968	0.997
Average F-measure	0.982	0.9964	0.9965

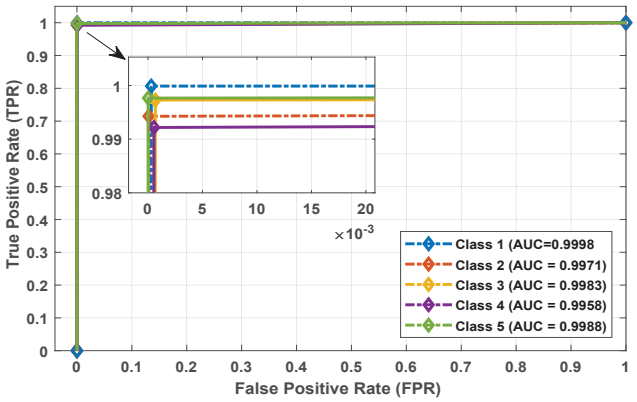
A. Stratified cross validation-based evaluation

In this subsection, we present the stratified k-fold cross validation (K=10)-based evaluation of the proposed classification models. Note that this method performs stratified sampling of given datasets instead of random sampling to provide the generalized performance of classifiers. Table III presents the promising performance of these classifiers with the computed AR, AP, and AF of around 98.2% for M1, and 99.6% for M2 and M3. Further, the computed accuracy during the stratified cross validation is above 99.6% for these classifiers while the model 2 showing the higher accuracy of 99.877%. We have also computed the receiver operating characteristics (ROC) to determine the trade-off between true positive rate (TPR), also known as sensitivity, and false positive rate (FPR) on a numerical scale. Fig. 9 illustrates the ROC plots of different classifiers with area under curve (AUC) of each class for the given classifier. The higher the AUC and closer the apex of the ROC curve towards the top left corner, as illustrated through the highlighted zoomed portion, greater the detection ability of a classifier for the given class. For example, Fig. 9 (a) presents

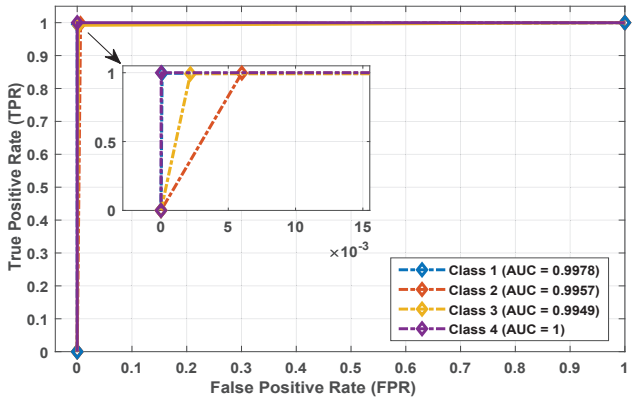
This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2021.3066316, IEEE Transactions on Smart Grid



(a) ROC plot of M1 classifier.



(b) ROC plot of M2 classifier.



(c) ROC plot of M3 classifier.

Fig. 9: ROC of different classifiers during the stratified k-fold cross validation

the ROC plot of M1 classifier where the ROC curve of class $z2$ is further to the top left corner with the computed AUC of 0.999, which shows higher detection ability for events in class $z2$ as compared to the remaining two classes.

B. Detection Performance under Noisy Environment

In this approach, a white Gaussian noise is injected in datasets by varying a signal to noise ratio (SNR) values from 30 dB to 70 dB in a step increase of 5 dB. Note that a higher value of SNR represents a lower level of noise in PMU measurements. Fig. 10 and Fig. 11 present the analysis in terms of average true positive rate (ATPR) and average false positive rate (AFPR) with an increase in SNR value from 30 dB to 70 dB for VMD-DT and DT algorithms. While it is intuitive to expect a low accuracy rate during a high noise level, the proposed VMD-DT algorithm still shows a consistent performance with 93% ATPR for M1, 98% ATPR for M2, and 93.8% ATPR for M3 for the lower SNR value of 30 dB. Unlikely to the high accuracy rate of VMD-DT, the performance of the DT is gradually degrading with a decrease in the value of SNR, where the ATPR of DT reduces to 82% for M1, 53.5% for M2, and 74.7% for M3 for the lower SNR value of 30 dB, as shown in Fig. 10. Similarly, it is evident from Fig. 11 that the computed AFPR is always lower than 2% for M1, 0.3% for M2, and 3.5% for M3 for the proposed VMD-DT algorithm. Note that the main reason behind the consistent and robust performance of VMD-DT is its close relationship with a wiener filtering technique that removes unwanted noises while updating modes.

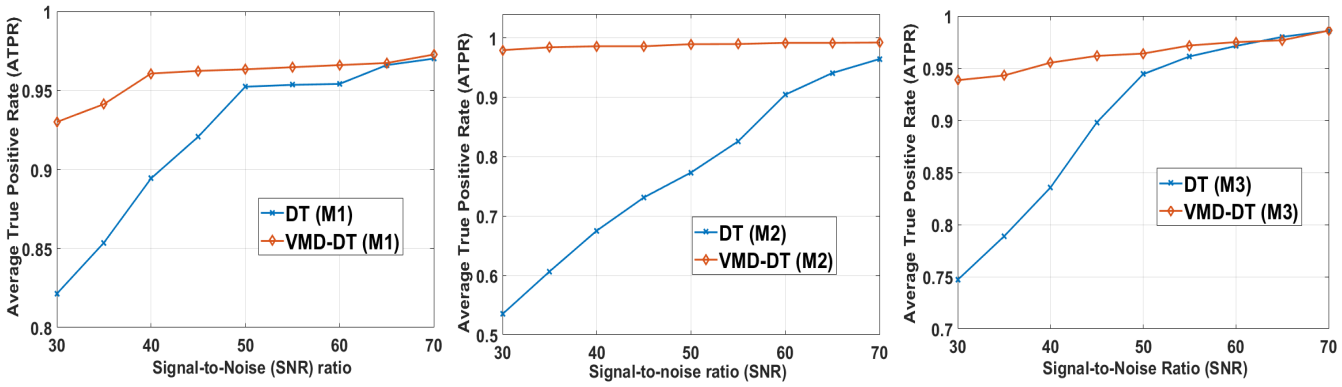
C. Processing Time

Fig. 12 presents the computational processing time (μs per PMU frame) of M1, M2, and M3 during testing. We observe that the average and maximum computational processing time of DT are 1.7665 μs and 10.049 μs that are almost similar to the VMD-DT's processing time, which are 2.4085 μs and 8.6498 μs. Also, during the real-time data processing of VMD-DT algorithm for different models, a sliding window of 300 samples (N_s) is assigned. The computed maximum computational processing time for total frames is around 2.6 ms, which is much lesser than a time step of incoming PMU packets (60 frames/sec) that are also further delayed by processing, concentrators, multiplexing and transducers, and the combined delay is estimated to be around 75 ms [37]. Additionally, the communication delay for fiber optics can be assumed to be about 25 ms [37]. Therefore, we can consider the total delay of 100-130 ms for incoming PMU packets. Since the synchrophasor-based CRAS has a timing requirement of around 200-300 ms [7], [8], the proposed ADS with a maximum cumulative response time of around 130 ms does not hamper the regular operation of CRAS.

VI. Conclusion

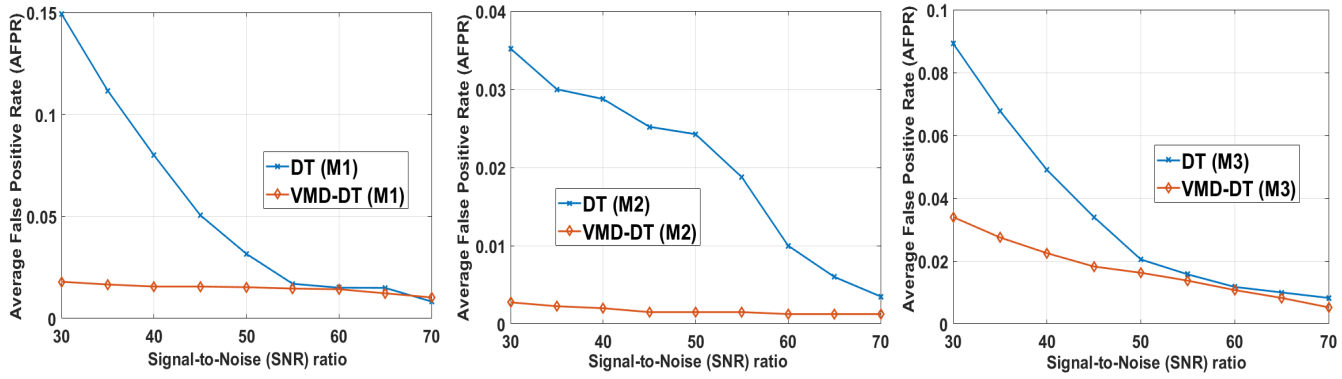
In this paper, we presented a machine learning-based CPADS using a multi-source heterogeneous system data, including PMU measurements and network properties, to detect data integrity and communication failure attacks in CRAS cyber-physical security. We described the proposed architecture and detection methodology that utilize DT and VMD algorithms to develop three classification models and final events identification is performed using a rules-based decision logic. We also described the rules-based features selection method and showcased its significance in selecting relevant features and enhancing the performance of classifiers. For detailed case studies, we utilized the IEEE 39 bus system and outlined several steps involved in generating datasets, data-preprocessing, and training and testing proposed models in the HIL cyber-physical testbed environment. Our experimental results showed that the proposed classification models of CPADS demonstrate better efficiency than other classifiers and also exhibit consistent performance during noisy PMU

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2021.3066316, IEEE Transactions on Smart Grid



(a) (b) (c)

Fig. 10: Variation of ATPR with SNR for model 1 (a), model 2 (b), and model 3 (c)



(a) (b) (c)

Fig. 11: Variation of AFPR with SNR for model 1 (a), model 2 (b), and model 3 (c)

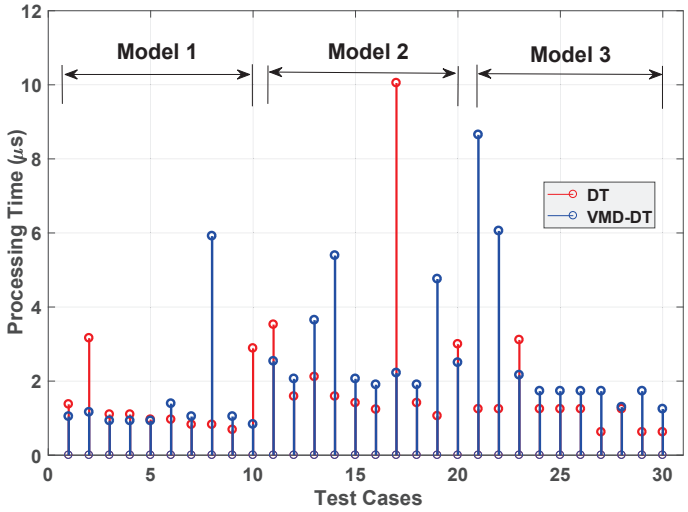


Fig. 12: Processing time (μs) for M1, M2, and M3

measurements. We also analyzed the computational processing time of these classifiers to make sure that the proposed CPADS can be integrated seamlessly with the existing CRAS. A potential avenue for future work is to develop a hybrid CPADS that combines rules, behavior, and online machine learning and deep learning-based approaches to enhance the cyberattack resiliency of CRAS.

ACKNOWLEDGMENT

This research is funded in part by US NSF Grant CNS 1446831, and US DOE Grant DE-OE0000830.

REFERENCES

[1] A. Ashok et al., "Cyber-Physical Attack-Resilient Wide-Area Monitoring, Protection, and Control for the Power Grid," in Proceedings of the IEEE, vol. 105, no. 7, pp. 1389-1407, July 2017.

[2] NERC Critical Infrastructure Protection Committee (CIPC), "cyber attack Task Force (CATF) Update," North American Electric Reliability Corporation (NERC), Dec. 2011.

[3] N. Falliere et al., "W32.stuxnet dossier," Technical report, Symantec, Feb. 2011.

[4] ICS-CERT, "cyberattack Against Ukranian Critical Insfrastructure.

[5] V. Madami et al., "Design and implementation of wide area special protection schemes," 57th Annual Conference for Protective Relay Engineers, 2004, College Station, TX, USA, 2004, pp. 392-402.

[6] M. Begovic et al., "Wide-Area Protection and Emergency Control," in Proceedings of the IEEE, vol. 93, no. 5, pp. 876-891, May 2005.

[7] The Anatomy of a Centralized Remedial Action System: What can be done in 50 milliseconds?

[8] J. Wen et al., "Evolution Pathway Towards Wide Area Monitoring and Protection—A Real-World Implementation of Centralized RAS System," in IEEE Transactions on Smart Grid, vol. 5, pp. 1506-1513, 2014.

[9] NERC Reliability Guideline: PMU placement and Installation, December 2016.

[10] C. W. Taylor, D. C. Erickson, K. E. Martin, R. E. Wilson and V. Venkatasubramanian, "WACS-Wide-Area Stability and Voltage Control System: RD and Online Demonstration," in Proceedings of the IEEE, vol. 93, no. 5, pp. 892-906, May 2005.

[11] I. Kamwa et al., "Catastrophe Predictors From Ensemble Decision-Tree Learning of Wide-Area Severity Indices,"in IEEE Transactions on Smart Grid, vol. 1, no. 2, pp. 144-158, Sept. 2010.

[12] F. Hashiesh, H. E. Mostafa, A. Khatib, I. Helal and M. M. Mansour, "An Intelligent Wide Area Synchrophasor Based System for Predicting and Mitigating Transient Instabilities," in IEEE Transactions on Smart Grid, vol. 3, no. 2, pp. 645-652, June 2012.

[13] Yi Zhang and K. Tomsovic, "Adaptive remedial action scheme based on transient energy analysis," IEEE PES Power Systems Conference and Exposition, 2004., New York, NY, 2004, pp. 925-931 vol.2.

[14] A. Hahn et al., Cyber-physical security testbeds: Architecture, application and evaluation for smart grid, Smart Grid, IEEE Transactions on, vol. 4, no. 2, pp. 847855, 2013.

[15] V. Kumar Singh, A. Ozen and M. Govindarasu, "Stealthy cyber attacks and impact analysis on wide-area protection of smart grid," 2016 North American Power Symposium (NAPS), Denver, CO, 2016, pp. 1-6.

[16] V. K. Singh and M. Govindarasu, "Decision Tree Based Anomaly Detection for Remedial Action Scheme in Smart Grid using PMU Data," 2018 IEEE PESGM, Portland, OR, 2018, pp. 1-5.

[17] S. Sridhar and M. Govindarasu, "Model-Based Attack Detection and Mitigation for Automatic Generation Control," in IEEE Transactions on Smart Grid, vol. 5, no. 2, pp. 580-591, March 2014.

[18] A. Ashok et al., "Online Detection of Stealthy False Data Injection Attacks in Power System State Estimation," in IEEE Transactions on Smart Grid, vol. 9, no. 3, pp. 1636-1646, May 2018.

[19] M. S. Rahman et al., "Multi-agent approach for enhancing security of protection schemes in cyber-physical energy systems," IEEE Transactions on Industrial Informatics, vol. 13, no. 2, pp. 436–447, April 2017.

[20] P. Wang and M. Govindarasu, "Multi-Agent Based Attack-Resilient System Integrity Protection for Smart Grid," in IEEE Transactions on Smart Grid, vol. 11, no. 4, pp. 3447-3456, July 2020.

[21] Y. Yang et al., "Multidimensional Intrusion Detection System for IEC 61850-Based SCADA Networks," in IEEE Transactions on Power Delivery, vol. 32, no. 2, pp. 1068-1078, April 2017.

[22] Y. Yang et al., "Intrusion Detection System for network security in synchrophasor systems," IET International Conference on Information and Communications Technologies (IETICT 2013), Beijing, China, 2013, pp. 246-252.

[23] V. K. Singh et al., "Security Evaluation of Two Intrusion Detection Systems in Smart Grid SCADA Environment," 2018 North American Power Symposium (NAPS), Fargo, ND, 2018, pp. 1-6.

[24] S. Brahma, R. Kavasseri, H. Cao, N. R. Chaudhuri, T. Alexopoulos and Y. Cui, "Real-Time Identification of Dynamic Events in Power Systems Using PMU Data, and Potential Applications—Models, Promises, and Challenges," in IEEE Transactions on Power Delivery, vol. 32, no. 1, pp. 294-301, Feb. 2017.

[25] M. Zhou, Y. Wang, A. K. Srivastava, Y. Wu, and P. Banerjee, "Ensemblebased algorithm for synchrophasor data anomaly detection," IEEE Transactions on Smart Grid, vol. 10, no. 3, pp. 2979–2988, May 2019.

[26] S. Matthews and A. St. Leger, "Leveraging mapreduce and synchrophasors for real-time anomaly detection in the smart grid," IEEE Transactions on Emerging Topics in Computing, pp. 1–1, 2019

[27] S. Pan, T. Morris and U. Adhikari, "Developing a Hybrid Intrusion Detection System Using Data Mining for Power Systems," in IEEE Transactions on Smart Grid, vol. 6, no. 6, pp. 3104-3113, Nov. 2015.

[28] A. Samui and S. R. Samantaray, "Assessment of ROCPAD Relay for Islanding Detection in Distributed Generation," in IEEE Transactions on Smart Grid, vol. 2, no. 2, pp. 391-398, June 2011.

[29] P. K. Dash, S. R. Samantaray and G. Panda, "Fault Classification and Section Identification of an Advanced Series-Compensated Transmission Line Using Support Vector Machine," in IEEE Transactions on Power Delivery, vol. 22, no. 1, pp. 67-73, Jan. 2007.

[30] M. K. Jena, S. R. Samantaray and L. Tripathy, "Decision tree-induced fuzzy rule-based differential relaying for transmission line including unified power flow controller and wind-farms," in IET Generation, Transmission Distribution, vol. 8, no. 12, pp. 2144-2152, 12 2014,

[31] K. Dragomiretskiy et. al, "Variational Mode Decomposition," in IEEE Transactions on Signal Processing, vol. 62, no. 3, pp. 531-544, 2014.

[32] P. D. Achlerkar et al., "Variational Mode Decomposition and Decision Tree Based Detection and Classification of Power Quality Disturbances in Grid-Connected Distributed Generation System," in IEEE Tran. on Smart Grid, July 2018.

[33] C. Dou, D. Wu, D. Yue, B. Jin and S. Xu, "A hybrid method for false data injection attack detection in smart grid based on variational mode decomposition and OS-ELM," in CSEE Journal of Power and Energy Systems.

[34] NERC, Remedial Action Development Definition Development project 2010-05.2 Special Protection System.

[35] National Electric Sector Cybersecurity Organization Resource, "Electric sector failure scenarios and impact analyses," Electric Power Research Institute, Tech. Rep. 2.0, Jun. 2014.

[36] Hall, M. (1999). Correlation based feature selection for machine learning. Doctoral dissertation, University of Waikato.

[37] M. M. Eissa et al., "A novel back up wide area protection technique for power transmission grids using phasor measurement unit," IEEE Trans. Power Del., vol. 25, no. 1, pp. 270–278, Jan. 2010.

Vivek Kumar Singh (Member, IEEE) received the B.E. degree in electrical engineering from the National Institute of Technology (NIT) Durgapur, India in 2014, the M.Eng. degree from the Iowa State University (ISU), and the Ph.D. degree in electrical engineering with a co-major in computer engineering from the ISU in 2020. He is currently a Postdoctoral Research Associate in the Department of Power and Energy Systems at Idaho National Laboratory (INL), Idaho Falls, US. His research interests include cyber-physical security for smart grid, wide-area monitoring, protection, and control (WAMPAC) applications, synchrophasor applications in power system, and smart-grid cyber-physical federation testbeds.

Manimaran Govindarasu (Fellow, IEEE) is currently the Anson Marston Distinguished Professor in Engineering and Mehl Professor of Computer Engineering in the Department of Electrical and Computer Engineering at Iowa State University. He received his Ph.D degree in Computer Science and Engineering from the Indian Institute of Technology (IIT), Madras, India in 1998. He has been on the faculty of Iowa State University since 1999. His research experiences are in the areas of cyber-physical system (CPS) security for the smart grid, cyber security, real-time systems and networks, and Internet of Things. He has co-authored 200 peer-reviewed research publications, and has given several invited talks and tutorials at reputed IEEE conferences, and delivered nearly two dozen training sessions and shortcourses on the subject of cybersecurity for the power grid. At Iowa State, he has built a CPS security testbed for smart grid and demonstrated several realistic attack-defense use-cases, and made the testbed accessible to RD community. He is a co-author of the text "Resource Management in Realtime Systems and Networks," MIT Press, 2001. He served as a Guest CoEditor for several flagship IEEE publications (IEEE Network, IEEE Power Energy, IEEE Trans. on Secure and Dependable Computing), and served as an Associate Editor for IEEE Transactions on Smart Grid and IEEE Transactions on Mobile Computing. He currently serves as the Chair of Cybersecurity Working Group within IEEE Power Energy Society AMPS Committee. He is a Fellow of the IEEE.